UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA HUNTINGTON

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH GOOGLE ACCOUNT jeremiahtaylor447@gmail.com that is stored at premises controlled by Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 24043	**Criminal No. 3:19-mj-00077** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael Moyer, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since January 2016. Upon getting hired by the Federal Bureau of Investigation, I received twenty weeks of training at Quantico, VA at the FBI Academy. As part of my training I learned how to conduct logical investigations into criminal activity. I was also trained in conducting logical investigations into counter-terrorism and counter-intelligence matters. I have specific training and experience conducting investigations into matters involving child exploitation and child pornography.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to acts of Violent Crime and Violent Crimes Against Children, to include but not limited to rape, sexual assault, child sexual assault and child pornography. I have participated in the execution of multiple federal search warrants in child exploitation and child pornography investigations.

3. This affidavit is made in support of an application for a warrant to search, pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain account(s) that are stored at the premises owned, maintained,

controlled, or operated by Google, a free web-based electronic mail service provider located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The account to be searched is **jeremiahtaylor447@gmail.com** (hereinafter, "Subject Account"), which is further described in Attachment A. As set forth below, there is probable cause to believe that in the account there exist evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e) are located in the Subject Account.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that one or more violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e) has been committed by JEREMIAH TAYLOR. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. See also 18 U.S.C. §§ 2703(a), (b)(1)(A),

and (c)(1)(A). Specifically, the Court is "a district of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e) relating to distribution of child pornography and attempted production of child pornography.

a. Title 18 U.S.C. § 2251(a) and (e) prohibit any person from employing, using, persuading, inducing, enticing or coercing, or attempting to employ, use, persuade, induce, entice or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, when the visual depiction travels in interstate or foreign commerce or the visual depiction was produced using materials that have traveled in interstate or foreign commerce.

b. Title 18 U.S.C. § 2252(a)(1) prohibits any person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of a minor engaging in sexually explicit conduct.

c. Title 18 U.S.C. § 2252(a)(2) prohibits any person from knowingly receiving or distributing, by computer or mail, any visual depiction of a minor engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of a minor engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

d. Title 18 U.S.C. § 2252A(a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

e. Title 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

f. Title 18 U.S.C. § 2252A(a)(3) prohibits any person from knowingly possessing or reproducing child pornography for distribution through

the mail or in interstate or foreign commerce by any means, including by computer.

g. Title 18 U.S.C. § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate and foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this affidavit and its attachments.

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where:

i. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. "File Transfer Protocol" (FTP) is a protocol that defines how files are transferred from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-locations of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.

i. "Mobile applications" as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

BACKGROUND INFORMATION ON GOOGLE

9. Based on my experience and information available from Google's website (google.com), I have learned the following information about Google and Gmail:

a. Google offers a collection of Internet-based services, including email and online data storage, which is owned and controlled by Google. The services are available at no cost to Internet users, though there are certain options, such as additional online data storage, that users may elect to pay money to receive. Subscribers obtain an account by registering on the Internet with

Google and providing Google with basic information, including name, gender, zip code, and other personal/biographical information. Subscribers are given a Google account which ends in "@gmail.com" which is utilized to access these online services.

b. Google maintains electronic records pertaining to the individuals and entities who maintain Google online subscriber accounts. These records often include account access information, email transaction information, account application information, and in some circumstances billing and payment information.

c. Any email that is sent to a Google online account subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Google. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely.

d. When a subscriber sends an email, it is initiated by the user, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google online account users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email may remain on the system indefinitely.

e. Google online account subscribers can store files, including but not limited to emails, documents, and image files, on servers maintained and/or owned by Google.

f. Google online account subscribers can also utilize a feature known as "History" that allows a user to track various historical account activity, including past Google Internet searches performed, information regarding devices which have been used to login to the Google online account, and physical location information regarding from where the Google online account was accessed.

g. Google keeps records that can reveal accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

10. Among the specific services offered by Google, I have learned the following:

a. **Google Drive**: Google online account subscribers can store files, including but not limited to emails, documents, and image files, on servers maintained and/or owned by Google. The online data storage service is known as

"Google Drive." According to Google, Google Drive provides users with "15 GB of free Google online storage, so you can keep photos, stories, designs, drawings, recordings, videos – anything." Further, according to Google, files in a Google Drive account "can be reached from any smartphone, tablet, or computer. So wherever you go, your files follow." In addition, according to Google, Google Drive allows users to share files by allowing others to "view, download, and collaborate on all the files you want–no email attachment needed."

b. **Google Hangouts**: According to Google, Google Hangouts "keeps you connected no matter where you are." Google Hangouts allows Google account users to:

i. Make one-to-one and group video calls that include up to ten people;

ii. Make phone calls using Wi-Fi or cellular data;

iii. Send text messages and group chats for up to 150 people; and

iv. Communicate with others regardless of devices (e.g., Android, iOS, and the web), and sync chats across all of a user's devices.

c. **Google Docs**: According to Google, Google Docs is a free-online document management application that allows users to create, edit, and access documents from their phone, tablet, and computer. Further according to Google, Google Docs allows users to, among other things: (a) work both on and off line; (b) to share documents, edit in real-time, and to chat and comment; (c) automatically save their work as it saves as a user types; (d) track revision history so that a user can see old versions of the same document sorted by date and who made the change; and (e) take advantage of pre-made documents and templates.

d. **Google Voice:** Google Voice is a telephony application that provides a user calling features "no matter what kind of phone [the user has] or which carrier [the user uses]." By using Google Voice, a user can, among other things:

i. Have a Google Voice number that will allow a user to have one number for all of the user's devices, which allows for all of the devices to ring simultaneously upon the Google Voice number being dialed;

ii. Choose a Google Voice number with a specific area code of the user's choosing or a number that spells out words;

iii. Have a Google Voice number that will stay the same regardless of whether the user moves, or changes carriers or devices;

iv. Automatic voice mail message transcription, including sending the transcription to the user's email account;

v. Receiving SMS or text messages on the user's device, in the Google Voice account, and in the user's email account;

vi. International calls for "low rates";

vii. Call blocking;

viii. Call screening that allows a user to listen to a voicemail being left in real time and accept the call while the message is being left; and

ix. Conference calling.

11. Further, Google typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service used, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, Google often has records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify the computers or other devices used to access the email account.

12. In addition, Google collects device-specific information, such as a user's hardware model, operating system version, unique device identifiers, and mobile network information including phone number. Google states it also may collect and process information about a user's

location, based on IP address, GPS, and other sensors that, for example, may provide Google with information on nearby devices, Wi-Fi access points and cell towers.

13. Therefore, the computers of Google are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and account application.

14. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow Google to make a digital copy of the entire contents of the information subject to seizure specified in Attachments A and identified with specificity in Attachment B. That copy will be provided to me or to any authorized federal agent for analysis and review pursuant to this search warrant and its Attachments.

15. Regarding searches of Google accounts in particular, based on my experience, and conversations with other experienced agents, I have learned that:

a. Individuals involved in computer crimes, such as phishing, may use Google searches to learn information about the targets of the emails, as well as background information used in creating the fictitious emails (e.g., information about the purported sender, or the content of the message). Additionally, Google searches for non-criminal topics (e.g., driving directions or searches for locations in one's neighborhood) can reveal information about the identity of the user of the account. As a result, a warrant for Google search history can provide valuable investigative information about the identity of the person who drafted or sent the phishing email.

b. Search warrants for location information stored by Google, when viewed in combination with email and search term results, can help to identify the user of the account by correlating the messages and search terms with the user's location at specific times. For example, location information can show the

locations the user frequented (e.g., home, work, school) at certain times, which can help differentiate that person from other individuals, even those who might live in the same home or work at the same office.

c. Individuals may store large quantities of files in Google Drive, including files that they send or receive through Gmail. Additionally, if an individual views attachments to Gmail messages through certain Google apps, Google may retain the file itself in Google Drive. Google Drive also allows users to collaborate with others in creating, editing, or sharing files. As such, it can produce investigative leads concerning co-conspirators, or others who may be aware of the activities of the account's user.

BACKGROUND REGARDING TECHNOLOGY, CHILD PORNOGRAPHY AND THE INTERNET

16. I have experience in the investigation of computer-related crimes. Based on my experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market

it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

CHARACTERISTICS OF PERSONS WHO COLLECT OR TRAFFIC CHILD PORNOGRAPHY

17. Your affiant has experience in assisting with, and leading, investigations into child pornography. Your affiant has conducted investigations into those who solicit and share child pornography by electronic means. Your affiant has worked with other law enforcement agencies to conduct logical investigations into those who solicit, share and otherwise engage in activity related to child pornography.

18. As a result of the aforementioned knowledge and experience, your affiant has learned that the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to, photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books and other media stored electronically on computers, digital devices or related digital storage media.

19. Offenders who deal with the above-referenced material depicting minors engaged in sexually explicit conduct obtain or traffic in such materials through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks (including from websites, peer-to-peer file sharing networks, news groups, electronic bulletin boards, chat rooms, instant message conversations, internet relay chats, email).

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.

c. Trading with other persons with similar interests through electronic transfer, shipments or deliveries.

20. These offenders collect materials depicting minors engaged in sexually explicit conduct for many reasons. These reasons include the following:

a. For sexual arousal and sexual gratification.

b. To facilitate sexual fantasies in the same manner that other persons utilize adult pornography.

c. As a medium of exchange in return for new images and video depicting minors engaged in sexually explicit conduct.

21. These offenders often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Subsequently, these offenders prefer not to be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft or damage. To safeguard their illicit materials, these offenders may employ the following methods:

a. The use of Internet-based data storage services, such a Google Drive.

b. The use of labels containing false, misleading or no title.

c. The application of technologies, software and other electronic means such as encryption, steganography (the practice of concealing a file, message, image, or video within another file, message, image, or video), partitioned hard drives, and misleading or purposefully-disguised applications on electronic devices.

d. The use of safes, safety deposit boxes or other locked or concealed compartments within premises or structures that the offender controls.

BACKGROUND INFORMATION ON KIK MESSENGER

22. Kik Messenger ("Kik") is a free, instant messaging application, developed by Kik Interactive, Inc. a company based in Waterloo, Canada. Kik may be accessed via various mobile devices, including iOS, Android and BlackBerry. Kik allows users to text, chat and share

photographs, videos, and other information with other Kik users. Kik uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos or videos.

23. When creating a Kik account, users are required to provide basic contact and personal identifying information. The information may include the user's full name, birth date, contact e-mail address, Kik password, screen names, and other personal identifiers. Email addresses can be "confirmed," which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or "unconfirmed," which means the email address is invalid, or the user did not click on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process. During this process, the user selects/creates a Kik user name. This user name is a unique identifier which can never be replicated.

24. Kik provides a platform for finding people who are available to chat and have similar interests. Users can send out an open invitation, search for specific users, or seek out new friends based on their profile details, by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Kik and can exchange communications or view each other's posted information.

PROBABLE CAUSE

25. On January 19, 2019, an FBI Online Covert Employee (hereinafter "OCE") connected to the Internet in an online undercover capacity from a computer located at the FBI Office in Salt Lake City, Utah. A software program was used to record the online activity, chats and images identified within Kik. Shortly before this date, the OCE posted numerous online bulletin messages on specific social media forums, which, based on the OCE's experience and information gathered from other sources, are websites frequented by individuals who have a sexual

interest in children and incest. The OCE responded to certain messages or post messages on these public forums and provided the OCE's Kik screen name.

26. Between January 19, 2019 and January 24, 2019, an individual with the Kik profile username "**58thatdude58**," identified as JEREMIAH TAYLOR, messaged the OCE on Kik. The OCE determined that "**58thatdude58**" appeared to have sexual interests in children and incest and was a member of a child pornography group titled "No.limits.-Yo.uN.G, #ta.boo.stuf" where group members posted thousands of images and videos of child pornography. "**58thatdude58**" posted links directly to the group that contained child pornography and also sent the OCE videos depicting child rape. The videos depict toddlers and/or prepubescent minors engaged in sexual acts. "**58thatdude58**" also expressed interest in wanting to produce child pornography of the OCE'S fictitious nine year-old daughter when he asked the OCE to take videos of his daughter naked and in sexual positions.

27. JEREMIAH TAYLOR was identified as "**58thatdude58**" through Kik subscriber data. The Kik subscriber data shows that the email associated with "**58thatdude58**" is **jeremiahtaylor447@gmail.com**. Subscriber data obtained through an administrative subpoena to Google shows that the email address **jeremiahtaylor447@gmail.com** belongs to JEREMIAH TAYLOR.

28. The recovery email address associated with **jeremiahtaylor447@gmail.com** is **taylor447@live.marshall.edu**. Through additional investigation, your affiant has learned that JEREMIAH TAYLOR is a former student of Marshall University in Huntington, West Virginia. JEREMIAH TAYLOR played football at Marshall University and his jersey number was 58. This jersey number corresponds to the 58 featured in the Kik username "**58thatdude58**."

29. Your affiant has learned that at the time of the chats, JEREMIAH TAYLOR was 30 years old and he was a resident of Ohio. This information matches the identifiers provided by "**58thatdude58**" during one of the conversations wherein he told the OCE that he was 30 years old and resided in Ohio.

30. Through the Kik subscriber data, your affiant has learned that "**58thatdude58**" accessed the Kik account during the conversations at issue using the IP address 74.195.15.79. Through investigation, your affiant has also learned that this IP address belongs to Suddenlink Communications, an Internet service provider. An administrative subpoena sent to Suddenlink Communications identifies the subscriber data for the IP address as Snap Fitness, 305 E. Main St. Milton, Cabell County, West Virginia 25541.

31. Your affiant located a LinkedIn profile for JEREMIAH TAYLOR. This profile bears a photograph depicting JEREMIAH TAYLOR's face and states that he is a graduate of Marshall University. It also states that JEREMIAH TAYLOR was an employee at Snap Fitness from July 2017 through July 2019, which includes the January 19, 2019 and January 24, 2019 time period of the Kik messages between "**58thatdude58**" and the OCE.

32. On or about October 4, 2019, your affiant spoke with a representative of Snap Fitness in Milton, West Virginia, and that individual confirmed that a JEREMIAH TAYLOR was previously employed at Snap Fitness in early 2019 but no longer works there.

33. Based on my experience in computer-related investigations, I believe that a search of the Subject Account, **jeremiahtaylor447@gmail.com,** will likely yield investigative leads relating to violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e).

INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A), requiring Google LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized personnel will perform a review of the data to locate the items described in Attachment B.

CONCLUSION

35. Based on the aforementioned factual information, as well as my training and experience, your affiant respectfully submits that there is probable cause to believe that the user of the Gmail/Google Drive account **jeremiahtaylor447@gmail.com** committed the offenses of distributing child pornography and attempting to produce child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e), and that evidence of those offenses, as more fully described in Attachment B, is presently contained in the Gmail/Google Drive account located on the computer system or server in the control of Google LLC at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

36. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

FURTHER AFFIANT SAYETH NOT.

Respectfully submitted,

MICHAEL MOYER
Special Agent
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me this 6th day of December, 2019.

HON. CHERYL A. EIFERT
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA

ATTACHMENT A

This warrant applies to information associated with the Google account corresponding to the email **jeremiahtaylor447@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

I. INFORMATION TO BE DISCLOSED BY GOOGLE LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC, which are stored at premises owned, maintained, controlled, or operated by Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, Google LLC is required to disclose to the Government information associated with the following Gmail/Google Drive account, for the time period from **January 19, 2019, through December 1, 2019**:

jeremiahtaylor447@gmail.com

1. All available Google account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve;

2. The contents of all emails and instant messages stored in the specified account, including copies of emails to and from the account, the source and destination addresses associated with each email or instant message, the date and time at which each email or instant message was sent, the size and length of each email or instant message;

3. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above;

4. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

5. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, change history, activity logs, device logs, and detailed billing and payment records;

6. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above;

7. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history;

8. All existing printouts from original storage of all the electronic mail described above;

9. All account contents previously preserved by Google, in electronic or printed form, including all e-mail, including attachments thereto, and Google Drive stored electronic files for the account described above);

10. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above;

11. All associated YouTube viewing history, uploading history, and other content; and

12. All location information stored in the Google account;

13. All records or other information regarding the identification of the email or instant messaging account, including the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with the account as well as corresponding session times and dates, account status, alternative email addresses provided during registration or throughout the account's duration of existence, methods of connecting, and log files; and

14. All records pertaining to communications between Google LLC and any person regarding the account, including contacts with support services and records of actions taken.

Pursuant to 18 U.S.C. § 2703(d), the service provider is hereby ordered to disclose the above information to the Government **within 14 days of service of this warrant**.

II. INFORMATION TO BE SEIZED BY THE GOVERNMENT

All information described above in Attachment A that constitutes fruits, evidence, and instrumentalities concerning violations of Title 18, United States Code, Sections 2252A(a)(2) and 18 USC 2251(a) and (e), including but not limited to, for each account identified in Attachment A, information pertaining to the following matters:

a. The distribution, possession, production, receipt, transfer of child pornography or visual depictions involving the use of a minor engaging in sexually explicit conduct, or the access with intent to view such materials;

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identity and whereabouts.

ADDENDUM TO ATTACHMENT B

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section II of Attachment B according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

1. Searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

2. Surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein;

3. Opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein; and/or

4. Performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto.